How Prime Compositing Can Be Made More Efficient and Useful than Mersenne Prime Method

30 September 2022
Simon Edwards
Research Acceleration Initiative

Introduction

As security researchers struggle to grasp the nature of the challenge posed by the advent of quantum computing, particularly where it relates to public key cryptography, the role of primes will once again come into focus. The current conventional wisdom holds that we must, at all costs, find the largest possible primes and if we skip 98% of the primes in the universe to get there, so be it.

This way of thinking may well be misguided for reason that, for one thing, using a variety of large exponents within a single algorithm is far more useful in building QC-resistant security than having a single ultra-large exponent at the heart of an algorithm. Secondly, there are many discernible patterns in the evolution of primes that make it possible to efficiently guess at non-Mersenne primes and fill in the gaps left by a quest to pick the low-hanging Mersenne fruit.

Abstract

It is only by catching up the non-Mersenne wavefront to the Mersenne wavefront that we may begin to demonstrate that next-in-series primes may be predicted with high accuracy from the list of established primes. The math that makes this possible is not much more complicated than the concept of scientific notation or the fact that multiples of five always end in a five or zero.

In prime compositing, which is already a respected and established method for searching for non-Mersenne primes, the next prime number may always be found by taking the highest known prime and adding to it a carefully selected smaller prime (or two) to generate a new prime. Candidates then have to be tested and either ruled in or out.

Many do not want to "waste their time" searching for these comparatively small primes, but this is largely a result of the current brute force approach to prime composite candidate selection. A more targeted approach would allow for most non-Mersennes to be found quickly with few wasted attempts (Mersenne requires hundreds of thousands of failed attempts to find a single valid prime) and would ultimately allow for all potential primes to be found without skipping any. For the non-Mersenne search to proceed, it is imperative that none be skipped. Having a more robust library of non-Mersenne primes to choose from for cryptographic purposes would be a boon for cybersecurity generally.

The relationship between primes and the ability to composite them is analogous to the way in which decimal places make modern arithmetic possible. Putting individual numbers from zero through nine next to each other in that system allows for larger numbers to be invented endlessly

without actually having to expand the library numerals in our system.

Just as this is so, primes can be composited (compositing being defined as simply adding two or more known primes together and then testing them for primeness) to create larger primes at will with little need for wasteful bruteforcing.

As prime numbers grow, the absolute number by which their value leaps tends to alternate according to a brownian-like motion in which the amount of increase tends to alternate unpredictably but is confined to what stock traders would call a "channel movement." In a channel movement, a stock price or other numerical variable oscillates somewhat predictably between minimum and maximum values based upon the recent history of the system.

Many looking for Mersenne primes take advantage of these patterns and make intelligent guesses about where the next prime in the Mersenne sequence lies. It is worth noting, however, that by skipping over so many primes, any intelligent guess as to a Mersenne prime's potential range is made more challenging than it needs to be.

As I will illustrate in the table below, the primes needed to make other primes (two-digit primes) are highly predictable. At each step, the only thing necessary is to take the previous prime in the sequence and add to it the right prime from early on in the sequence. Which number that is tends to grow along the same exact trendline as the primes themselves. Observe:

1
2 (1+1)
3 (2+1)
5 (3+2)
7 (5+2)
11 (7+3+1)
13 (11+2)
17 (13+5)
19 (17+2)
23 (19+3+1)
29 (23+7)

and a larger example:

3931
3943 (3931+7+5)
3967 (3943+23+2)

The first prime to composite is always a certainty in this method; it is always the most recently confirmed and generally largest prime.

The next step is to implement what might be termed a wheeling method wherein the various primes composited are of different scales, but tend to grow at the same rate. That growth rate starts out at exactly n (1.2) for each five primes traversed but is halved at ten such cycles, halved again by the end

of 100 such cycles, and so long. With the number five forming the basis of these cycles, the halvings are at 5, 50, 500, 5000, and so on.

Since we already know the basic pattern of prime evolution, we can plug in educated guesses based upon that prime evolution to each wheeling variable. As long as all primes prior to the one you are solving for have been found, you should have a pretty good idea where the position of each wheel should be. It is also worth noting in the two-digit examples that it is every 5th prime that is a composite of three as opposed to two. The need to be composited from three is generally a direct result of the increase in the size of that prime being noticeably larger than the previous incremental increase. These large jumps tend to happen on every fifth prime, although even this rule is not absolute.

The numbers needed to composite the next prime will always consist of the largest known prime added to either one or two additional primes. Those primes, in turn, can be predicted based upon which primes were composited to find the previous prime. Their evolution, it bears repeating, mirrors the evolution of the primes themselves. The wheeled primes needed to find a new prime will swing up and down in precisely the same pattern as the primes generally.

What is meant by swing up and down? The difference between one prime and the next in the sequence can either increase relative to the previous increase or it can decrease. Although each prime is larger than the last, the amount of increase in that value, though it straddles a median line slowly trending upward, tends to follow the brownian-like motion mentioned earlier. Remarkably, it seems that when primes that are, for instance, larger than average jumps, are involved in a compositing operation, the needed prime to aid in computing the next prime will tend to plunge for the next time. More than a mere tendency, these alternations, although unpredictable when computing initial primes, are, in terms of their relative short-period increase or decrease, in lockstep with the original run when they are used as factors to build the next prime.

Conclusion

This means, profoundly, that we can, more or less, predict the next primes in the sequence and efficiently fill in the non-Mersenne gaps in the body of known primes.